Apex A - Z of Cyber Security

Introduction

Welcome to your Apex A-Z of cyber security. Over the next 26 slides, we are going to outline the most important and relevant cyber security elements for you and your business.

This concise guide is relevant to all business employees, so feel free to forward to colleagues. As always, should you have any questions, then please do get in touch:

Laser House, Media Village, Waterfront Quay,
Salford Quays, M50 3XW.

https://w3w.co/blur.beside.spoken

T: 0161 233 0099
E: enquiries@apexcomputing.co.uk

AntiVirus or EDR (Next-generation AntiVirus) should be installed on every device as a first line of defence.

Antivirus is a software program designed to detect, prevent, and remove malicious software or malware from a computer system. Malware refers to any software that is intentionally designed to harm, steal, or damage computer systems, data, or networks.

Antivirus software typically scans the computer's files and memory for known malware signatures, as well as behaviour that may indicate the presence of new and previously unknown threats. When an antivirus detects malware, it will typically quarantine or remove the infected files to prevent further damage to the system. Antivirus software can also provide real-time protection by monitoring system activity and blocking potential threats in real-time.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

Bitlocker is Windows' internal Encryption system – devices should always be encrypted as it protects your data in case of a machine being lost/stolen.

BitLocker is a built-in encryption feature in Microsoft Windows operating systems that provides enhanced security for data stored on a computer's hard drive or other storage devices. It uses advanced encryption technology to protect the contents of the disk, which helps prevent unauthorised access to sensitive information.

BitLocker works by encrypting the entire hard drive, including the operating system and user data. It uses a password, a smart card, or a recovery key to access the encrypted data. Without the proper key or password, the data is inaccessible, even if someone removes the hard drive from the computer and tries to read it using another system.

BitLocker is commonly used by organizations and individuals who require a high level of security for their data, such as those in the financial, healthcare, and legal industries. It can also be used to protect personal data on laptops and other portable devices that may be lost or stolen.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

Check everything! If an email/call asks for confidential data, always double check with someone else before actioning the request.

Anyone can easily be tricked into revealing confidential information or disclosing data – so, always double and triple check the identity of the sender and ask for a second opinion.

Cybersecurity is important because it helps protect computer systems, networks, and data from unauthorized access, theft, and damage caused by cyberattacks. In today's digital age, where most businesses and individuals rely heavily on technology, cybersecurity has become essential to safeguard personal and sensitive information from cybercriminals who seek to exploit vulnerabilities in computer systems and networks

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

DKIM and DMARC can help further protect your email setup. Contact your Customer Relationship Manager to ask about us configuring this on your tenant.

DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting, and Conformance) are email authentication technologies that help to prevent email spoofing and phishing attacks

Together, DKIM and DMARC provide a powerful email authentication system that can help protect against spam, phishing, and other email-based attacks. By authenticating the source of an email message and verifying its integrity, these technologies help to ensure that legitimate emails are delivered to their intended recipients, while malicious emails are blocked or flagged for further review.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

E

Emails are the most common way for attacks to enter your network.

Once again, always check and verify the identity of the person that has sent you the email. Check for any misspellings or questionable email sender addresses:

Emails can be vulnerable to hacking if the proper security measures are not in place. There are several ways that hackers can gain unauthorized access to emails, such as:

Password cracking: Hackers can use software to crack or guess your password.
Phishing: Hackers can send you fraudulent emails that look legitimate, tricking you into clicking on links or downloading attachments that contain malware.
Man-in-the-middle attacks: Hackers can intercept and modify emails while they're being transmitted over a network.

Malware: Hackers can send you emails with attachments that contain malware, which can compromise your system when you open the attachment.

To reduce the risk of email hacking, it's important to use strong and unique passwords, enable two-factor authentication, avoid clicking on links or downloading attachments from unknown sources, and keep your antivirus software up to date. It's also essential to use secure email providers that offer strong encryption and other security features to protect your emails.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex
Computing Services

Firewalls protect your network by limiting what can come into your network.

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a private network and the public internet, preventing unauthorized access and protecting the network from malicious traffic.

They work by analysing packets of data that are transmitted over a network connection. When a packet of data attempts to enter or leave the network, the firewall examines it to determine whether it meets the predefined security criteria. If the packet is deemed safe, it is allowed to pass through the firewall and continue to its destination. If the packet is deemed unsafe or suspicious, the firewall can either block it or quarantine it for further analysis.

Firewalls are an essential component of any network security infrastructure, and they help to protect organizations from a wide range of threats, including hackers, viruses, and other malicious actors.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

Geofencing – this means only allowing access to your systems from designated locations, whether this is an IP address or a country.

Geofencing is a cyber security feature that identifies the geographic region where traffic originates. It does this by looking at the IP address of incoming traffic or network requests, each of which is tied to a physical location.

If you run a U.K. business and wanted to block any network traffic from China, for example, geofencing would allow you to create a firewall policy to do this.

But geofencing goes beyond just blocking traffic and it can be used for other security policies as well. For example, you could set up a geofencing policy that only allows access to your server/CCTV from the UK. This prevent users being able to brute-force logins from other countries.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

Hacking isn't just done by bored teenagers anymore – There are whole companies whose "job" is to gain access to your network.

Hacking is the act of exploiting weaknesses in computer systems or networks in order to gain unauthorised access or control. Hackers use a variety of techniques to exploit vulnerabilities in software, hardware, and human behaviour to gain access to sensitive information, disrupt services, or cause damage to the targeted system

Basic IT security such as strong passwords and antivirus are simple ways to prevent hacking of your IT systems.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex
Computing Services

Incident Reporting – always let us know if you think something has happened with your network security.

The team at Apex are on hand 24/7/365 to help should your network or systems be compromised. We are also on hand to advise and to supply the equipment and solutions needed to protect your IT infrastructure.

Reporting any incident in good time is also vital, to ensure that all the necessary and required steps can be taken to protect your systems.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex
Computing Services

Jargon can often make Cyber Security seem impossible or difficult to understand – if you need help understanding anything, don't hesitate to reach out to Apex.

Take a look at our Jargon Buster feature on the Apex website news page – we asked our customers what terms and jargon confused them so our handy jargon buster guide can help! Don't worry – even though the Apex team are highly qualified tech experts – we still speak to our customers in plain English!

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex
Computing Services

K

Keep your devices safe – don't leave devices in your car, or on an unattended table.

We have all made the mistake of leaving our phone or bag in a taxi, however, keeping your personal belongings safe means keeping them secure!

You are less likely to encounter a breach if you keep your devices safe at all times and locked when not in use.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

Lock your screen when you leave your machine.

Or, simply press the Windows key and ‘L’ on your computer keyboard. By locking your screen, you will prevent anybody from accessing your system and its data.

It is very easy to just get up and walk away from your desk to make a coffee, but it is still vital that you lock your devices and carry your phone with you.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

MFA (Multi Factor Authentication) – enable this everywhere it is available.

MFA stands for Multi-Factor Authentication. It is a security mechanism that requires users to provide two or more forms of authentication in order to access a system or an application.

The first factor is typically a username and password, which is something the user knows. The second factor can be something the user has, such as a security token or a smartphone with an authenticator app, or something the user is, such as a fingerprint or facial recognition.

MFA is an effective way to enhance security because it adds an extra layer of protection against unauthorised access, even if the user's password is compromised. If a hacker obtains a user's password, they still need to provide the additional factor to gain access to the system.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

Network Access Control – make sure you only allow access to files from trusted sources/devices.

Network access control is the act of keeping unauthorized users and devices out of a private network. Organizations that give certain devices or users from outside of the organization occasional access to the network can use network access control to ensure that these devices meet corporate security compliance regulations.

This can help to protect your data by only allowing access to file servers/shares from devices that you know and trust.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

One-Time Passcode – a type of MFA option that provides a code for you to put in for additional verification – commonly as an app on your phone.

This is yet another added level of security for your devices and systems. It may take you a couple of extra seconds to log in, but those seconds are time well spent, to ensure the safety and security of your IT infrastructure and network.

A one-time passcode (OTP) is a temporary code that is generated for use in a single login session or transaction. OTPs are often used as a second-factor authentication method to enhance the security of online accounts, transactions, or services.

OTP works by generating a unique code that is sent to the user's registered mobile phone number or email address. The user then enters this code into the login or transaction page, and it is verified to authenticate the user. OTPs are typically valid for only a short period, usually ranging from a few seconds to a few minutes, after which they expire and become invalid.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

Passwords should be strong, unique, and over 12 digits. If you can't remember them all, use a password manager.

Have a read of our blog feature on the Apex website news page, where we discuss the importance of having a strong password and using a password manager. Once again, this is another added level of security designed to protect you and your organisation.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex
Computing Services

Qualifications such as Cyber Essentials and ISO 27001 help your business meet recognised Security Baselines.

Cyber Essentials is a UK government-backed scheme that provides a set of basic technical security controls to help organisations protect against common cyber threats. The scheme outlines five essential areas of cybersecurity.

1. Boundary firewalls and internet gateways: protecting against unauthorised access to an organisation's network.

2. Secure configuration: ensuring that systems are configured securely and are kept up to date.

3. Access control: controlling who has access to information and systems and ensuring that access is only granted to those that need it.

4. Malware protection: protecting against malware, including viruses and spyware.

5. Patch management: keeping software up to date with the latest security patches.

CYBER ESSENTIALS PLUS

Information Security Management ISO 27001 Certified

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

Ransomware is one of the biggest threats for all companies, with around 500 million attacks happening in 2022.

Ransomware is a type of malicious software (malware) that is designed to block access to a computer system or data until a ransom is paid. Ransomware typically encrypts the victim's files, rendering them inaccessible, and demands payment in exchange for the decryption key needed to restore access to the files.

Ransomware is often distributed through phishing emails, malicious websites, or as part of a larger malware attack. Once installed on a victim's system, the ransomware will typically display a message or pop-up window informing the victim of the attack and demanding payment in exchange for the decryption key. The payment is often demanded in cryptocurrency, such as Bitcoin, to make it difficult to trace.

Ransomware attacks can be devastating, as they can cause permanent loss of important data and disrupt business operations. Prevention is key, and users can protect themselves by practicing good cyber hygiene, such as regularly backing up data, keeping software up-to-date, and being cautious of suspicious emails and links.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

S

Sandbox – this is the name of an external machine that acts as a testing environment for software/attachments to make sure they're not malicious.

A sandbox is a security mechanism that isolates applications or processes from the rest of the system to prevent them from causing harm or accessing sensitive information. A sandbox creates a controlled environment where an application or process can be tested or run without affecting the rest of the system.

Sandboxing is commonly used in software development to test new applications or updates without risking damage to the system. Sandboxing is also used in security to isolate potentially malicious code or files, such as attachments in emails or files downloaded from the internet, and to analyse them in a safe and controlled environment before allowing them to run on the system.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex
Computing Services

Train your users on Security Policies and Procedures.

Training is vital for your team so that they can identify and prevent cyber security threats. Here at Apex, our highly skilled cyber security team can assist you and help you organisation to find the right level of training and support for your organisation. Give us a quick call to discuss any IT training requirements that you may have...

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex
Computing Services

Updates for all software/systems should be installed ASAP.

By allowing updates to your devices and systems, you are enabling the latest security features and programs to protect your systems and infrastructure. Most devices will tell you when an update is required, and many are automatic.

You can allow updates to run in the background while you are able to continue with going about your daily tasks!

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

V

VPNs should always be used when accessing Company Data while outside of the office.

VPN stands for Virtual Private Network. It is a technology that creates a secure and encrypted connection between a user's device and a remote server on the internet. VPNs are commonly used to protect online privacy and security, and to bypass internet censorship and geo-restrictions.

When a user connects to a VPN, their device creates a secure and encrypted tunnel to the VPN server. All internet traffic from the user's device is then routed through this tunnel to the VPN server, which acts as a proxy for the user's internet connection. This makes it difficult for anyone to intercept or monitor the user's online activities, and can help protect sensitive information such as passwords, credit card numbers, and personal data.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

WiFi – Never connect to “open” or “unsecured” wireless hotspots. Only connect to networks you know and trust – attackers can sit on open networks and collect your data.

As tempting as it can be – avoid accessing these ‘open’ or ‘unsecured’ WiFi networks. Similarly, make sure to lock down and password protect your own WiFi network.

Unsecured Wi-Fi networks can be dangerous because they allow anyone within range to access the network and potentially compromise the security of devices connected to the network. An unsecured Wi-Fi network does not require a password or encryption to access, which means that anyone with a Wi-Fi enabled device can connect to the network without authorisation.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

X-Rated content should be blocked from your company network. These sites are often filled with malware and malicious links/ adverts.

You can install content filters across your organisation's network. content filter is a software or hardware solution that is designed to restrict or block access to certain types of content on the internet. Content filters are commonly used by organizations to enforce internet usage policies and to protect users from accessing inappropriate or harmful content.

Content filters can be configured to block access to specific websites, web pages, or types of content, such as gambling, pornography, or social media.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

Y

You are the last line of defence.

Yes, you! That means ensuring that you and your team have the right training in place and that everybody is aware of how to spot and prevent cyber threats. You are only as strong as your weakest link as they say!

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex
Computing Services

Zero Trust is the future! The Zero Trust model means you inherently distrust anything you don't know about – treat everything as a threat...

Apex Zero Trust is a security software solution that is designed to provide advanced application whitelisting and control to prevent malware and unauthorized applications from running on endpoints.

Application whitelisting is a security technique that allows only approved applications to run on a system, while blocking all other applications. Apex Zero Trust uses a 'zero-trust' approach to application whitelisting, meaning that all applications are blocked by default, and only authorized applications that have been explicitly approved by an administrator are allowed to run. This approach provides an additional layer of protection against malware and other threats that may evade traditional antivirus or firewall solutions.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

apex Computing Services

Summary

We hope you have found this A-Z guide of interest! Apex are best placed to advise and assist you and your business with all things cyber security.

Cyber security is a vital element for any business of any size. For a free cyber security audit, please get in touch:

Laser House, Media Village, Waterfront Quay,
Salford Quays, M50 3XW.

https://w3w.co/blur.beside.spoken

T: 0161 233 0099
E: enquiries@apexcomputing.co.uk